REMARKS

In response to the Office Action dated April 24, 2007, Applicants respectfully request reconsideration and withdrawal of the rejections of the claims.

Claim 1 was rejected under the second paragraph of 35 U.S.C. § 112. The Office Action objects to the use of the term "critical instruction", stating that the specification does not provide a standard for ascertaining the meaning of this term. Applicants respectfully traverse this assertion. At page 8, lines 7-10, the specification explains that critical instructions are those which manipulate a target bit in a differential power analysis. Further descriptions of critical instructions can be found in the specification, for example, at page 17, lines 11-15, and page 18, lines 28-30. It is respectfully submitted that, upon reviewing the specification as a whole, a person of ordinary skill in the art would be readily apprised of the types of instructions that fall within the term "critical instruction".

In any event, to remove the issue, references to "critical instructions" have been deleted from the claims.

Claims 1 and 6-15 were rejected under 35 U.S.C. § 102, on the basis of the Kocher patent (US 6,278,783). Claims 2 and 5 were rejected under 35 U.S.C. § 103, on the basis of the Kocher patent, and claims 3 and 4 were rejected on the basis of the Kocher patent in view of the Luyster patent (US 6,182,216). For the reasons presented hereinafter, it is respectfully submitted that the Kocher patent does not anticipate, nor otherwise suggest, the subject matter of the pending claims, whether considered by itself or in combination with the Luyster patent.

The Kocher patent, like the present invention, is concerned with an attacker's ability to derive secure information by observing a series of operations performed in a cryptographic system. However, the approach that is employed in the Kocher patent is substantially different from the claimed invention. Specifically, the Kocher patent discloses a technique wherein the message to be encrypted, and/or the encryption keys, are disguised, or "blinded", prior to processing by the DES algorithm. This blinding is accomplished by generating two values which, when combined with one another by means of an exclusive-OR operation, result in the original message, or keys. Permutation of these values are employed to perform the encryption. See, for example, column 6, lines 28-38 of the Kocher patent.

In contrast, the claimed subject matter provides a countermeasure against attacks on the security of cryptographic information by introducing randomness into the operations that are performed during the execution of the cryptographic algorithm. Referring to Figure 3 of the application, one of the standard operations that is performed in each round of the DES algorithm is known as the SBOX operation, in which a 48-bit input value is converted into a 32-bit output value. This conversion is implemented by means of a table, an example of which is illustrated in Figure 6 of the application. Typically, the same table is employed in each of the 16 rounds of the DES algorithm.

In accordance with the claimed invention, a countermeasure is provided by using different tables during different rounds of the algorithm. After one table is established for the algorithm, another table is generated by performing an exclusive-OR operation on components of the first table, using a random value. As illustrated in the exemplary

embodiment of Figure 7, one of the tables (TC_1) is used for some of the rounds of the algorithm, and the other table (TC_2) is used during other rounds of the algorithm.

It is respectfully submitted that the Kocher patent does not disclose, nor otherwise suggest, such a technique as a countermeasure against attacks on the security of cryptographic information. Claim1 recites a countermeasure method, wherein at least some of the rounds of a cryptographic algorithm are implemented with a first manipulating means that supplies an output data item from an input data item. In rejecting claim 1, the Office Action refers to the Kocher patent at column 6, lines 39-42 as disclosing this feature. This cited passage describes the manner in which the blinded values for the cryptographic key K are produced. It is not apparent from the Office Action what feature disclosed in this passage is considered to constitute the claimed manipulating means, that provides an output data item from an input data item.

Claim 1 goes on to recite that at least one other round of the cryptographic algorithm is implemented with other manipulation means for supplying output data, wherein the other manipulation means are obtained from the first manipulation means by performing an exclusive-OR operation with a random value. Thus, the second, or "other", manipulation means is derived from the first manipulation means, by performing an exclusive-OR operation on it. Since it is not apparent what feature described in the Kocher patent is considered to correspond to the claimed first manipulating means, it is also not apparent how the reference is being interpreted to disclose the other manipulating means that is derived from the first manipulating means by performing an exclusive-OR operation with a random value.

If the rejection based upon the Kocher patent is not withdrawn, the Examiner is respectfully requested to identify, with particularity, what feature in the patent is being interpreted as the first manipulating means, and where the patent discloses obtaining another manipulating means by performing an exclusive-OR operation on the first manipulating means.

Claim 1 recites that at least one of the multiple rounds of the cryptographic algorithm is implemented with the first manipulating means, and at least one other round of the algorithm is implemented with the other manipulation means. Hence, the claim explicitly recites that different manipulation means are employed in different respective rounds of the algorithm. It is respectfully submitted that the Kocher patent does not disclose this subject matter. Rather, it appears that the same blinded values are employed throughout the entire DES algorithm. There is no disclosure that suggests employing different operations during different respective rounds of the algorithm.

Claim 7 explicitly recites that the manipulation means are tables of constants. In rejecting this claim, the Office Action refers to the Kocher patent at column 7, lines 16-65. It appears that the Office Action is referring to the S table described therein. However, the Office Action does not correlate this description with the passages that were cited in the rejection of claim 1. Specifically, in rejecting claim 1, the Office Action refers to the Kocher patent at column 6, lines 39-42, in connection with the claimed manipulating means. This passage does not relate to the S table. Consequently, the rejection of claim 7 is inconsistent with the interpretation that was provided in rejecting claim 1.

Furthermore, the Kocher patent does not disclose multiple S tables that are respectively used during different rounds of the DES algorithm. Nor does it describe the derivation of one S table from another S table, by performing an exclusive-OR operation with a random value. Rather, the passage recited in column 7 pertains to the initialization of parameters, including the S table. It does not, however, disclose the generation of different S tables to be implemented during different rounds of the DES algorithm.

For at least these reasons, therefore, it is respectfully submitted that the subject matter of claim 1 is not anticipated by the Kocher patent. For these same reasons, claim 12 is likewise patentably distinct from the reference. Furthermore, since all other claims depend, directly or indirectly, from either claim 1 or claim 12, they are likewise not anticipated, nor otherwise suggested, by the Kocher patent, whether considered by itself or in combination with the Luyster patent.

Reconsideration and withdrawal of the rejections, and allowance of all pending claims is respectfully requested.

Applicants request an extension of time for one month, to and including August 24, 2007. Authorization to charge the fee for this extension to Deposit Account No. 02-4800 is being provided with the electronic filing of this response.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY, PC

By: /JamesLaBarre/
James A. LaBarre
Registration No. 28,632

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620

Date: August 24, 2007